

Meon Junior School
E-Safety and
Acceptable use of IT policy

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Other mobile devices with web functionality
- Gaming, especially online
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video Broadcasting

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements, usually 13 years.

At Meon Junior School, we understand the responsibility to educate our pupils on e Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact their department. Any ICT authorised staff member will be happy to comply with this request.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, emails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

Breaches

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, where appropriate, the Portsmouth Disciplinary Procedure.

Policy breaches may also lead to criminal or civil proceedings.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's Head teacher or IT leader. Additionally, all security breaches, lost/stolen equipment or data (including passwords and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported.

Acceptable Use Agreement: Pupils - Primary

Primary Pupil Acceptable Use Agreement / eSafety Rules

- I will only use ICT in school for school purposes.
- I will only use my class e-mail address or my own school email address when emailing.
- I will only open email attachments from people I know, or who my teacher has approved.
- I will not tell other people my IT passwords.
- I will use the features provided by Google APPs appropriately.
- I will only open/delete my own files.
- I will make sure that all IT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using IT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of IT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.

Dear Parent/ Carer

ICT including the internet, email and mobile technologies has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these e Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact Mr Hanna or Mrs Kershaw.

Parent/ carer signature

We have discussed this and(child name) agrees to follow the e Safety rules and to support the safe use of ICT at Meon Junior School.

I am give permission / do not give permission (delete as appropriate) for my child's photograph and work to be published on the school website (no names will be used)

Parent/ Carer Signature

Class Date

Acceptable Use Agreement: Staff, Governors and Visitors

Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Jackie Kershaw school IT leader or Luke Hanna, the Head teacher.

- I will only use the school's email / Internet / Intranet / website and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will use the features provided by Google Apps appropriately and understand that these features are subject to the same AUP, both within and outside of school.
- I will ensure that personal data (such as data held on SIMs software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not install any hardware or software without permission of the IT leader.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher. I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature Date

Full Name(printed)

Job title

Computer Viruses / Data Security

- All files downloaded from the Internet, received via email or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used
- Never interfere with any anti-virus software installed on school ICT equipment that you use
- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know
- The school gives relevant staff access to its Management Information System, with a unique username and password
- It is the responsibility of everyone to keep passwords secure
- Staff are aware of their responsibility when accessing school data
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used
- Anyone expecting a confidential or sensitive fax should notify the sender before it is sent.

e-Mail

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette; 'netiquette'. In order to achieve ICT level 4 or above, pupils must have experienced sending and receiving e-mails.

Managing e-Mail

- The school gives all staff their own email account to use for all school business as a work based tool This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses
- All emails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
- Staff sending emails to external organisations, parents or pupils are advised to cc. the Headteacher, line manager or designated account
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- Emails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:
 - Delete all e-mails of short-term value
 - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives
- All pupil email users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication, or arrange to meet anyone without specific permission, virus checking attachments
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail
- Staff must inform the IT leader or Head teacher if they receive an offensive e-mail

E Safety

E Safety - Roles and Responsibilities

As e Safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in this school is *Jackie Kershaw* who has been designated this role as IT lead. All members of the school community have been made aware of who holds this post.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home-school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHE .

E Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the pupils on a regular and meaningful basis. e Safety is embedded within our curriculum and we continually look for new opportunities to promote e Safety.

- The school has a framework for teaching internet skills in ICT/ PSHE lessons
- The school provides opportunities within a range of curriculum areas to teach about e Safety
- Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the eSafety curriculum
- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Cybermentors, Childline or CEOP report abuse button
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum

E Safety Skills Development for Staff

- New staff receive information on the school's acceptable use policy as part of their induction
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of e Safety and know what to do in the event of misuse of technology by any member of the school community
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas

Internet Access

The internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

Managing the Internet

- The school provides pupils with supervised and filtered access to Internet resources (where reasonable) through the school's fixed internet connectivity provided by EXA broadband and schools filter system.
- Staff will preview any recommended sites before use
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources
- All users must observe copyright of materials from electronic resources

Internet Use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience
- Do not reveal names of colleagues, pupils, others or any other confidential information acquired through your job on any social networking site or other online application
- On-line gambling or gaming is not allowed

It is at the Headteacher's discretion as to what internet activities are permissible for staff and pupils and how this is disseminated.

- Our school also employs some additional web-filtering through Google Apps for education, which is the responsibility of *the IT lead and Head teacher*.
- Meon Junior School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required
- The school does not allow pupils access to internet logs

- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the IT lead or teacher as appropriate
- It is the responsibility of the school, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from *the Headteacher/ IT leader*

Online technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavors to deny access to social networking and online games websites to pupils within school
- All pupils are advised to be cautious about the information given by others on such websites, for example users not being who they say they are
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)
- Our pupils are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online
- Our pupils are asked to report any incidents of Cyberbullying to the school
- Staff may only create blogs, wikis or other online areas in order to communicate with pupils using the school website or other systems approved by the Headteacher

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting e Safety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss e Safety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

- Parents/carers and pupils are actively encouraged to contribute to adjustments or reviews of the school e Safety policy by using the feedback form on our website
- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website)
- Parents/carers are expected to sign a Home School agreement containing the following statement or similar
 - **We will support the school approach to on-line safety and not deliberately upload or add any text, image, sound or videos that could upset or offend any member of the school community**
- The school disseminates information to parents relating to eSafety where appropriate in the form of;
 - Information and celebration evenings
 - Practical training sessions e.g. How to adjust the Facebook privacy settings
 - Posters
 - School website
 - Newsletter items

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and others without advance permission from the Headteacher
- Pupils and staff must have permission from the Headteacher before any image can be uploaded for publication

Consent of Adults Who Work at the School

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file

Publishing Pupil's Images and Work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, ie exhibition promoting the school
- general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc.

Parents or carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Only the Head teacher or IT lead has authority to upload to the site.

School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

School ICT Equipment

- As a user of the school ICT equipment, you are responsible for your activity
- It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school's inventory
- Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT facilities if available
- Ensure that all ICT equipment that you use is kept physically secure
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990
- It is imperative that you save your data on a frequent basis to the school's network. You are responsible for the backup and restoration of any of your data that is not held on the school's network
- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable device. If it is necessary to do so the local drive must be encrypted
- It is recommended that a time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles
- Privately owned ICT equipment should not be used on a school network
- On termination of employment, resignation or transfer, return all ICT equipment to your Manager. You must also provide details of all your system logons so that they can be disabled
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or

classified information is disclosed to any unauthorised person

Mobile Technologies

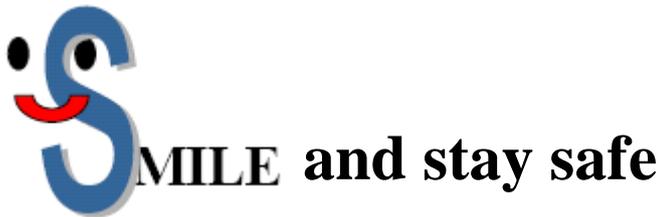
Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such as Smartphones, Blackberries, iPads, games players, are generally very familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/carer using their personal device
- Pupils are not allowed to bring personal mobile devices/phones to school but may send them to the office to be kept securely for the day.
- This technology may be used for educational purposes, as mutually agreed with the Headteacher. The device user, in this instance, must always ask the prior permission of the bill payer
- The school is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

Smile and Stay Safe Poster

eSafety guidelines to be displayed throughout the school



Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you

Information online can be untrue, biased or just inaccurate. Someone online may not be telling the truth about who they are - they may not be a 'friend'

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply

Social Media, including Facebook and Twitter

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

- Our school may use Facebook and Twitter to communicate with parents and carers. The Head teacher is responsible for all postings on these technologies and on Facebook monitors responses from others
- Staff are not permitted to access their personal social media accounts using school equipment at any time.
- Pupils are not permitted to access social media accounts whilst at school and we actively encourage parents to be responsible when setting up such systems and adhere to the age guidelines set. Any breach of this may be reported to the relevant body.
- Staff, governors, pupils, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others
- Whilst employees, governors, parents and carers are free to use the internet in this way, they must ensure that they do not breach the law or disclose Meon Junior School's confidential information, breach copyright, defame the school, its suppliers, partners, customers or other employees, or disclose personal data or information about any individual that could breach the Data Protection Act 1998 and to keep completely confidential any information regarding the children, their families or other staff which is learned through the School.
- Staff, governors, pupils, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever
- Staff, governors, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law

When writing a weblog and placing information on social networking sites, employees, governors, parents and carers should be careful not to:

- Include any information that breaches copyright and should link to other material rather than cutting and pasting it.
- Defame (libel) anyone. An employee, governor, parent or carer who makes a defamatory statement that is published on the internet may be legally liable for any damage to the reputation of the individual concerned.
- Include personal information about an individual without his / her consent, otherwise they risk breaching the Data Protection Act 1998, which is a criminal offence.
- Include material that is abusive, defamatory, sexist, racist or homophobic or that could be interpreted as harassment or bullying.
-
- Bring Meon Junior School into disrepute.

Google Apps for Education

The school also provides Google Apps for education as a facility used to enhance the IT learning experience and to ease work for pupils, staff and governors. We will provide students with Google Apps for Education accounts. Google Apps for Education includes free, web-based programs like email, document creation tools, shared calendars, and collaboration tools. This service is available through an agreement between Google and the Meon Junior School.

Google Apps for Education runs on an Internet domain purchased and owned by the school and is intended for educational use. Teachers will be using Google Apps for lessons, assignments, and communication.

Google Apps for Education is also available at home, the library, or anywhere with Internet access. School staff will monitor student use of Apps when students are at school. Parents are responsible for monitoring their child's use of Apps when accessing programs from home. Students are responsible for their own behavior at all times. These Services include Gmail, Google Calendar, Google Docs, Google Groups and Google Sites. Use of these Services is governed by the acceptable use policy. Google also has its own AUP which must also be adhered to, this is listed below.

Google Apps Acceptable Use Policy

Use of the Services is subject to this acceptable use policy ("AUP").

If not defined here, capitalized terms have the meaning stated in the applicable contract ("Agreement") between customer, reseller or other authorized user ("You") and Google.

You agree not to, and not to allow third parties or Your End Users, to use the Services:

- to generate or facilitate unsolicited bulk commercial email;
 - to violate, or encourage the violation of, the legal rights of others;
 - for any unlawful, invasive, infringing, defamatory, or fraudulent purpose;
 - to intentionally distribute viruses, worms, Trojan horses, corrupted files, hoaxes, or other items of a destructive or deceptive nature;
 - to interfere with the use of the Services, or the equipment used to provide the Services, by customers, authorized resellers, or other authorized users;
 - to alter, disable, interfere with or circumvent any aspect of the Services;
- to test or reverse-engineer the Services in order to find limitations, vulnerabilities or evade filtering capabilities;